

09/582797
526 Rec'd PCT/PTO 29 JUN 2000

Atty. Docket No.: 15675.P321
Express Mail #: EL634501798US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the application of:

Claude Meggle

For: A METHOD AND APPARATUS FOR PROCESSING CONFIDENTIAL CODES

REQUEST FOR PRIORITY

Hon. Commissioner of
Patents and Trademarks
Washington, D.C. 20231

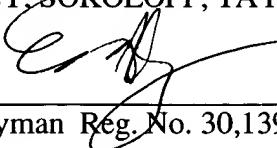
Dear Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely French Patent Application No. 97 16786 filed December 31, 1997.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 5/7/2000
By:
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800


Eric S. Hyman Reg. No. 30,139

THIS PAGE BLANK (USPTO)

08/582797

EU



REC'D 01 FEB 1999
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

PRIORITY DOCUMENT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **05 JAN. 1999**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

A handwritten signature in black ink, appearing to read 'Martine Planche', is placed over the typed title.

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIETE
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

This Page Blank (uspto)



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa

N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réserve à l'INPI

DATE DE REMISE DES PIÈCES

31 DEC 1997

N° D'ENREGISTREMENT NATIONAL

97 16786

DÉPARTEMENT DE DÉPÔT

fk

DATE DE DÉPÔT

31 DEC. 1997

2 DEMANDE Nature du titre de propriété industrielle

- brevet d'invention demande divisionnaire
 certificat d'utilité transformation d'une demande de brevet européen



1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET REGIMBEAU
26, Avenue Kléber
75116 PARIS

n° du pouvoir permanent références du correspondant téléphone

236853 D17250 FVR 01 45 00 92 02

date

certificat d'utilité n°

oui non

Établissement du rapport de recherche

différé immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

oui non

Titre de l'invention (200 caractères maximum)

Procédé et dispositif de traitement de codes confidentiels

3 DEMANDEUR (S) n° SIREN code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

Forme juridique

GROUPEMENT DES CARTES BANCAIRES

Nationalité (s) Française

Adresse (s) complète (s)

Pays

31, rue de Berri, Immeuble Monceau, 75008 PARIS

FR

En cas d'insuffisance de place, poursuivre sur papier libre

4 INVENTEUR (S) Les inventeurs sont les demandeurs oui non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES requise pour la 1ère fois requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire - n° d'inscription)

GG *dr-2*

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

JK

**DIVISION ADMINISTRATIVE DES BREVETS**

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE**DÉSIGNATION DE L'INVENTEUR**

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL**97 16786**

TITRE DE L'INVENTION : Procédé et dispositif de traitement de codes confidentiels

LE(S) SOUSSIGNÉ(S)

GROUPEMENT DES CARTES BANCAIRES
31, rue de Berri, Immeuble Monceau, 75008 PARIS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

MEGGLE Claude
104, boulevard Arago
75014 Paris, FR

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire**25 février 1998****CABINET REGIMBEAU**

L'invention concerne le domaine des dispositifs à codes et des procédés de traitement de codes. Plus précisément, l'invention concerne le domaine des systèmes avec code d'accès confidentiel, notamment, les dispositifs et procédés permettant de sécuriser l'accès à certaines opérations telles que des transactions, en particulier monétiques.

De nombreuses fonctions de sécurité utilisent un code confidentiel. Ce code, numérique, typiquement de 2 à 12 chiffres, associé à un profil d'identification de titulaire autorisé à détenir ce code, permet au titulaire d'utiliser certaines fonctions protégées, et seule la connaissance du code permet le déverrouillage des fonctions.

La généralisation de ce moyen d'authentification, notamment combinant code et carte à microprocesseur, entraîne le développement d'attaques lors desquelles le titulaire du code, sous la menace, est contraint de révéler son code.

Dans l'art antérieur, si le code entré dans le dispositif de sécurité est erroné, le dispositif (par exemple un guichet automatique de banque) en informe en clair la personne qui a saisi le code, généralement par affichage sur un écran. Ainsi, la personne qui a entré le code sait que le code entré est erroné et qu'il doit essayer un autre numéro que celui qu'il a composé précédemment. En général, le nombre d'essais autorisés est limité (trois est le plus fréquent), afin d'assurer une protection contre les tentatives systématiques.

Dans le cas d'une agression, l'agresseur est de cette façon, informé que le code qu'il a obtenu de sa victime est faux, ce qui peut l'inciter à devenir plus menaçant et plus dangereux.

Le but de l'invention est de fournir un dispositif et un procédé pour diminuer les risques encourus par le titulaire d'un code, victime de telles attaques, tout en conservant la protection des fonctions à protéger.

Ce but est atteint grâce à un procédé de traitement de codes confidentiels dans un système à fonctions sécurisées comprenant les étapes consistant à :

- recevoir un code ;
 - vérifier une première habilitation, conditionnée par un premier code, pour accéder à une première fonction ; et
 - autoriser l'accès à la première fonction si la première habilitation est
- 5 reconnué,
- caractérisé en ce qu'il comprend en outre, si la première habilitation n'est pas reconnue, l'étape consistant à :
- utiliser le code afin de vérifier une deuxième habilitation, conditionnée par un deuxième code distinct du premier code, pour
- 10 déclencher au moins une deuxième fonction en ne révélant pas le fait que le code ne permet pas d'obtenir la première habilitation.

De cette façon, la victime peut révéler à l'agresseur un deuxième code ; grâce au procédé selon l'invention, ce deuxième code est distingué d'un premier code, habilité pour accéder à une première fonction ; il n'y a

15 alors pas accès à la première fonction qui reste protégée ; mais ce deuxième code peut être habilité pour déclencher une deuxième fonction qui peut servir de leurre, destiné à détourner l'agresseur du projet d'accéder à la première fonction. L'agresseur détourné de son projet ne cherchera pas à menacer davantage sa victime pour qui les risques encourus se trouvent

20 par conséquent réduits.

Avantageusement, la première fonction du procédé selon l'invention est une transaction bancaire.

Avantageusement, les étapes du procédé selon l'invention, consistant à vérifier les première et deuxième habilitations, font intervenir

25 une carte à microprocesseur.

Avantageusement encore, l'étape de vérification de la deuxième habilitation du procédé selon l'invention comprend les opérations consistant à :

- obtenir un nouveau code, par une deuxième transformation inverse
- 30 d'une première transformation simple permettant au titulaire du premier code d'obtenir le deuxième code à partir du premier code ; et

- exécuter à nouveau l'étape de vérification de la première habilitation pour tester le nouveau code.

Avantageusement, ladite première transformation simple du procédé selon l'invention est réalisée par un décalage élémentaire d'un caractère du 5 premier code.

Avantageusement, le procédé selon l'invention, comprend en outre une étape d'invalidation, si l'étape consistant à vérifier la première habilitation a été testée plus d'un nombre déterminé de fois sans succès.

Avantageusement, la deuxième fonction, du procédé selon 10 l'invention, consiste à afficher un message choisi aléatoirement parmi plusieurs messages indiquant que l'accès à la première fonction n'est pas possible, sans toutefois spécifier que le code n'est pas celui permettant d'obtenir la première habilitation.

Avantageusement, la deuxième transformation simple du procédé 15 selon l'invention est fonction de paramètres accessibles sur la carte à microprocesseur.

Selon un autre aspect, l'invention est un dispositif de contrôle d'accès à des fonctions sécurisées, à code confidentiel, pour la mise en œuvre du procédé défini ci-dessus.

20 Avantageusement, ce dispositif comprend :

- des moyens pour recevoir un code ;

- des moyens pour vérifier avec ce code une première habilitation, conditionnée par un premier code, pour accéder à une première fonction ; et - des moyens pour autoriser l'accès à la première fonction si

25 l'habilitation est reconnue ;

il est caractérisé en ce qu'il comprend en outre

- des moyens pour utiliser, si l'accès à la première fonction est refusé, le code pour vérifier une deuxième habilitation conditionnée par un deuxième code, distinct du premier code, à déclencher au moins une

30 deuxième fonction en ne révélant pas le fait que le code ne permet pas d'obtenir la première habilitation.

Avantageusement, le dispositif selon l'invention est un terminal pour carte bancaire.

Avantageusement, le dispositif selon l'invention est utilisé pour sécuriser une transaction bancaire.

5 Avantageusement, les étapes consistant à vérifier les premières et deuxièmes habilitations font intervenir un profil d'utilisateur enregistré numériquement.

10 Avantageusement, les moyens du dispositif selon l'invention, pour vérifier les première et deuxième habilitations, font intervenir une carte à microprocesseur.

Avantageusement, les moyens du dispositif selon l'invention, pour vérifier la deuxième habilitation permettent les opérations consistant à :

15 - obtenir un nouveau code, par une deuxième transformation inverse d'une première transformation simple permettant au titulaire du premier code d'obtenir le deuxième code à partir du premier code ; et

- exécuter à nouveau l'étape de vérification de la première habilitation pour tester le nouveau code.

20 Avantageusement, ladite transformation simple du dispositif selon l'invention, est réalisée par un décalage élémentaire d'un caractère du premier code.

Avantageusement, le dispositif selon l'invention comprend en outre des moyens d'invalidation mis en œuvre si la première habilitation a été testée plus d'un nombre déterminé de fois sans succès.

25 Avantageusement, la deuxième fonction du dispositif selon l'invention est réalisée par des moyens qui affichent un message choisi aléatoirement parmi plusieurs messages indiquant que l'accès à la première fonction n'est pas possible, sans toutefois spécifier que le code n'est pas celui permettant d'obtenir la première habilitation.

30 Avantageusement, la deuxième transformation simple du dispositif selon l'invention est fonction de paramètres accessibles sur la carte à microprocesseur.

On comprendra mieux l'invention à l'aide de la description détaillée qui suit et des dessins joints sur lesquels :

- la figure 1 est un diagramme représentant schématiquement les principales unités composant un dispositif particulier pour la mise en œuvre 5 de l'invention ; et

- la figure 2 est un synopsis de l'ensemble des étapes d'un exemple de mise en œuvre du procédé selon l'invention.

Dans un mode privilégié, mais non limitatif, de réalisation du dispositif selon l'invention, celui-ci est un distributeur automatique de billets.

- 10 Comme représenté sur la figure 1, il comprend de façon classique en soi une unité centrale 1 qui traite et échange des informations avec un lecteur 2 de cartes bancaires 10, et un clavier 3 (ou tout autre dispositif interactif de saisie), pour commander un mécanisme distributeur 4 de billets, le lecteur 2 de cartes bancaires 10 et produire des messages affichés sur un écran 5.
- 15 Le traitement des informations et la commande des mécanismes composant le dispositif selon l'invention par l'unité centrale 1, s'appuie sur des échanges avec une unité de mémoire 6.

Une carte 10 est munie d'un microprocesseur. Ce microprocesseur correspond à un profil de titulaire autorisé à détenir un premier code.

- 20 Le titulaire détient aussi un deuxième code qui sera utilisé comme code de secours de la manière qui sera exposée plus loin.

L'utilisateur détient donc deux codes. Le premier code est son code confidentiel usuel, habilité pour accéder à une première fonction, en l'occurrence, pour l'exemple décrit ici, une transaction monétique du type 25 distribution automatique de billets.

Le deuxième code est un code de secours. Il peut être révélé par un utilisateur menacé par un agresseur à la place de son code confidentiel.

Ce deuxième code est facilement mémorisable et est obtenu par une première transformation arithmétique simple à partir du premier.

- 30 Préférentiellement, le deuxième code ne diffère du premier code que par un chiffre, lequel chiffre est avantageusement modifié seulement de

plus 1 ou moins 1 par rapport au chiffre de même rang dans les premier et deuxième codes.

Préférentiellement, aussi, le dispositif selon l'invention est mis en œuvre suivant le procédé suivant, décrit en référence en la figure 2.

5 Lorsqu'un utilisateur souhaite obtenir une première fonction 180, en l'occurrence la distribution de billets de la part du dispositif selon l'invention, il introduit sa carte 10 dans le lecteur 2 et compose un code sur le clavier 3.

L'unité centrale 1 commence alors au début 100 une procédure de test, avec des étapes se succédant comme indiqué ci-dessous.

10 Suit une étape de lecture du profil de l'utilisateur et de réinitialisation 105 du décompte du nombre de fois où le code est composé.

Un indicateur 110 témoignant du fait que le code n'a pas encore été transformé est généré.

Vient alors l'étape de saisie 115 du code.

15 Le code est testé, par un test de code 120 pour vérifier une première habilitation.

Si le test 120 donne un résultat négatif, c'est que le code fourni au dispositif selon l'invention ne correspond pas au premier code détenu par l'utilisateur, c'est à dire son code confidentiel. Un premier test d'indicateur

20 130 est alors effectué. Si l'indicateur témoigne du fait que le code n'a pas encore été transformé, l'unité centrale 1 engage un test de deuxième habilitation et procède à une dérivation 140 d'une deuxième transformation, inverse d'une première transformation simple permettant au titulaire d'un premier code d'obtenir un deuxième code (son code de secours) à partir du 25 premier code.

Un indicateur 145 témoignant du fait que la dérivation 140 a été effectuée, est généré.

Ce code obtenu par la dérivation 140 est utilisé pour reproduire l'étape de vérification de la première habilitation, au niveau du test de code 30 120. Si après la dérivation 140, le code obtenu ne correspond toujours pas au premier code (code confidentiel usuel), c'est que le code introduit au

début 100 n'était pas le deuxième code (code de secours). Il peut s'agir, par exemple, d'une erreur de frappe de la part de l'utilisateur. La procédure se poursuit en recommençant le premier test d'indicateur 130. Mais cette fois-ci, le test d'indicateur 130 détecte qu'une deuxième habilitation a déjà été testée (T=1). La procédure se poursuit donc par un traitement de code erroné 150 semblable à ceux connus de l'homme du métier. Plus particulièrement, un test du nombre de fois où le code a été composé 190 est effectué. Si ce nombre est égal à 3, par exemple, une étape d'invalidation 200 est effectuée pour mettre fin 210 à la procédure. Si ce nombre est inférieur à 3, il est demandé à l'utilisateur s'il souhaite un abandon 220 de la procédure. Si c'est le cas, la procédure prend fin 210, sinon le code doit être ressaisi après que l'indicateur 110 ait été réinitialisé.

Si le test de code 120 donne un résultat positif, un deuxième test 160 de l'indicateur est effectué. Si l'indicateur témoigne du fait que le code n'a pas été transformé, l'utilisateur a accès à la fonction protégée 180 (par exemple la distribution de billets). Si l'indicateur témoigne du fait que le code a déjà été transformé, c'est que le code ayant passé avec succès le test de première habilitation, avait préalablement subi la dérivation 140. Le code entré au début 100 de la procédure était donc le code de secours. La procédure se poursuit alors par une deuxième fonction 170, en l'occurrence, une transaction de secours 170, qui peut être une fonction leurre.

La deuxième fonction 170 correspond pour l'exemple décrit ici à une transaction de secours qui peut recouvrir plusieurs solutions.

Une solution peut consister à afficher sur l'écran 3, un message choisi aléatoirement parmi plusieurs messages indiquant que l'accès à la première fonction 180 n'est pas possible, sans toutefois spécifier que le code fourni au dispositif selon l'invention n'est pas celui permettant d'obtenir la première habilitation.

Par exemple, le message sera du type «transaction momentanément indisponible» ou «crédit insuffisant» ou encore n'importe quel autre des messages courants utilisés pour indiquer un incident de fonctionnement

d'un guichet automatique bancaire ou un dysfonctionnement du compte du titulaire.

- Selon une autre solution, la procédure normale de distribution de billets sera initiée, par exemple en demandant quelle somme est désirée, puis si 5 l'utilisateur souhaite un reçu, mais une panne sera simulée et la somme demandée ne sera pas délivrée.

Selon une autre solution, il sera délivré une somme, mais limitée, par exemple, à celle minimale pouvant être distribuée.

- Par ailleurs, la deuxième transformation 140 simple permet de retrouver 10 le premier code (code confidentiel usuel) à partir du deuxième code (code de secours). Avantageusement, cette deuxième transformation 140 simple est variable, en fonction par exemple de paramètres accessibles sur la carte à microprocesseur. Par exemple, pour un certain organisme bancaire, la deuxième transformation 140 peut consister à incrémenter de 1 le chiffre du 15 deuxième rang du code, alors que pour un autre organisme, la transformation consistera à retrancher une unité au chiffre du dernier rang. La deuxième transformation 140, et notamment le sens de variation sur un chiffre, peut aussi dépendre de la nature paire ou impaire du nombre constituant le «code de banque», le «code de guichet», etc.
- 20 De nombreuses autres possibilités peuvent être envisagées.

- Un autre avantage de l'invention dans sa forme décrite ci-dessus est qu'il n'est nécessaire de tester qu'un seul code au niveau du microprocesseur de la carte 10. Les cartes 10 utilisées actuellement sont donc compatibles avec cette forme de réalisation de l'invention et il n'est 25 aucunement nécessaire de changer les cartes 10 déjà en circulation.

- On comprendra tout de même qu'il est possible d'utiliser des cartes 10 permettant de tester le premier code et le deuxième code, indépendamment l'un de l'autre, et sans effectuer la deuxième transformation 140, sans s'écartez de l'esprit de l'invention.
- 30 On comprendra aussi qu'il a été utilisé pour la description détaillée ci-dessus l'exemple des dispositifs de type distributeur de billets, mais que

l'invention s'applique également aux terminaux de paiement par carte bancaire ainsi qu'à tout type de système à fonction sécurisée 180, comme certains dispositifs informatiques, certains sites militaires, industriels, etc..

Au lieu de tester le code composé en combinaison avec une carte 10 à 5 microprocesseur, pour accéder aux systèmes à fonction sécurisée 180, on peut envisager de le tester en combinaison avec un nom d'utilisateur, ou n'importe quel autre élément de profil d'utilisateur.

La deuxième fonction 170 décrite ci-dessus est une fonction de leurre simulant un dysfonctionnement du système à protéger. Il pourrait être 10 envisagé dans d'autres cas, comme deuxième fonction 170, le déclenchement d'un signal d'alerte, l'émission de gaz de défense, etc.

REVENDICATIONS

1. Procédé de traitement de codes confidentiels dans un système à fonctions sécurisées (180) comprenant les étapes consistant à :
 - recevoir un code ;
- 5 - vérifier une première habilitation, conditionnée par un premier code, pour accéder à une première fonction (180) ; et
 - autoriser l'accès à la première fonction (180) si la première habilitation est reconnue, caractérisé en ce qu'il comprend en outre, si la première habilitation n'est
- 10 pas reconnue, l'étape consistant à :
 - utiliser le code afin de vérifier une deuxième habilitation, conditionnée par un deuxième code distinct du premier code, pour déclencher au moins une deuxième fonction (170) en ne révélant pas le fait que le code ne permet pas d'obtenir la première habilitation.
- 15 2. Procédé selon la revendication 1, caractérisé par le fait que la première fonction (180) est une transaction bancaire.
3. Procédé selon l'une quelconque des revendications précédentes, caractérisé par le fait que les étapes consistant à vérifier les première et deuxième habilitations font intervenir un profil d'utilisateur enregistré
- 20 numériquement.
4. Procédé selon l'une quelconque des revendications précédentes, caractérisé par le fait que les étapes consistant à vérifier les première et deuxième habilitations, font intervenir une carte (10) à microprocesseur.
5. Procédé selon l'une quelconque des revendications précédentes,
- 25 caractérisé par le fait que l'étape de vérification de la deuxième habilitation comprend les opérations consistant à :
 - obtenir un nouveau code, par une deuxième transformation (140) inverse d'une première transformation simple permettant au titulaire du premier code d'obtenir le deuxième code à partir du premier code ; et
- 30 - exécuter à nouveau l'étape de vérification de la première habilitation pour tester le nouveau code.

6. Procédé selon la revendication 5, caractérisé par le fait que ladite première transformation simple est réalisée par un décalage élémentaire d'un caractère du premier code.

7. Procédé selon l'une quelconque des revendications précédentes, 5 caractérisé en ce qu'il comprend en outre une étape d'invalidation (200) si l'étape consistant à vérifier la première habilitation a été testée plus d'un nombre déterminé de fois sans succès.

8. Procédé selon l'une des revendications précédentes caractérisé par le fait que la deuxième fonction (170) consiste à afficher un message 10 choisi aléatoirement parmi plusieurs messages indiquant que l'accès à la première fonction (180) n'est pas possible, sans toutefois spécifier que le code n'est pas celui permettant d'obtenir la première habilitation.

9. Procédé selon l'une quelconque des revendications 5 à 8 caractérisé par le fait que la deuxième transformation (140) simple est 15 fonction de paramètres accessibles sur la carte (10) à microprocesseur.

10. Dispositif de contrôle d'accès à des fonctions sécurisées (180), à code pour la mise en œuvre du procédé selon l'une des revendications précédentes, comprenant :

20 - des moyens pour recevoir un code ;
- des moyens pour vérifier avec ce code une première habilitation, conditionnée par un premier code, pour accéder à une première fonction (180) ; et
- des moyens pour autoriser l'accès à la première fonction (180) si l'habilitation est reconnue,

25 caractérisé en ce qu'il comprend en outre :

- des moyens pour utiliser, si l'accès à la première fonction (180) est refusé, le code pour vérifier une deuxième habilitation conditionnée par un deuxième code distinct du premier code pour déclencher au moins une deuxième fonction (170) en ne révélant pas le fait que le code ne permet 30 pas d'obtenir la première habilitation.

11. Dispositif selon la revendication 10 caractérisé en ce qu'il est un

terminal pour carte bancaire.

12. Dispositif selon l'une quelconque des revendications 10 et 11, caractérisé par le fait qu'il est utilisé pour sécuriser une transaction bancaire.

5 13. Dispositif selon l'une quelconque des revendications 10 à 12, caractérisé par le fait que les moyens pour vérifier les première et deuxième habilitations, font intervenir une carte (10) à microprocesseur.

14. Dispositif selon l'une quelconque des revendications 10 à 13, caractérisé par le fait que les moyens pour vérifier la deuxième habilitation 10 permettent les opérations consistant à :

- obtenir un nouveau code, par une deuxième transformation (140) inverse d'une première transformation simple permettant au titulaire du premier code d'obtenir le deuxième code à partir du premier code ; et

15 - exécuter à nouveau l'étape de vérification de la première habilitation pour tester le nouveau code.

15. Dispositif selon la revendication 14, caractérisé par le fait que ladite première transformation simple est réalisée par un décalage élémentaire d'un caractère du premier code.

16. Dispositif selon l'une quelconque des revendications 10 à 15, 20 caractérisé en ce qu'il comprend en outre des moyens d'invalidation mis en œuvre si la première habilitation a été testée plus d'un nombre déterminé de fois sans succès.

17. Dispositif selon l'une quelconque des revendications 10 à 16, caractérisé par le fait que la deuxième fonction (170) est réalisée par des 25 moyens qui affichent un message choisi aléatoirement parmi plusieurs messages indiquant que l'accès à la première fonction (180) n'est pas possible, sans toutefois spécifier que le code n'est pas celui permettant d'obtenir la première habilitation.

18. Dispositif selon l'une quelconque des revendications 14 à 17, 30 caractérisé par le fait que la deuxième transformation (140) simple est fonction de paramètres accessibles sur la carte (10) à microprocesseur.

ORIGINAL

CABINET RECHERCHES
CONSEILS EN PROPRIÉTÉ INDUSTRIELLE

26, Avenue du Maréchal

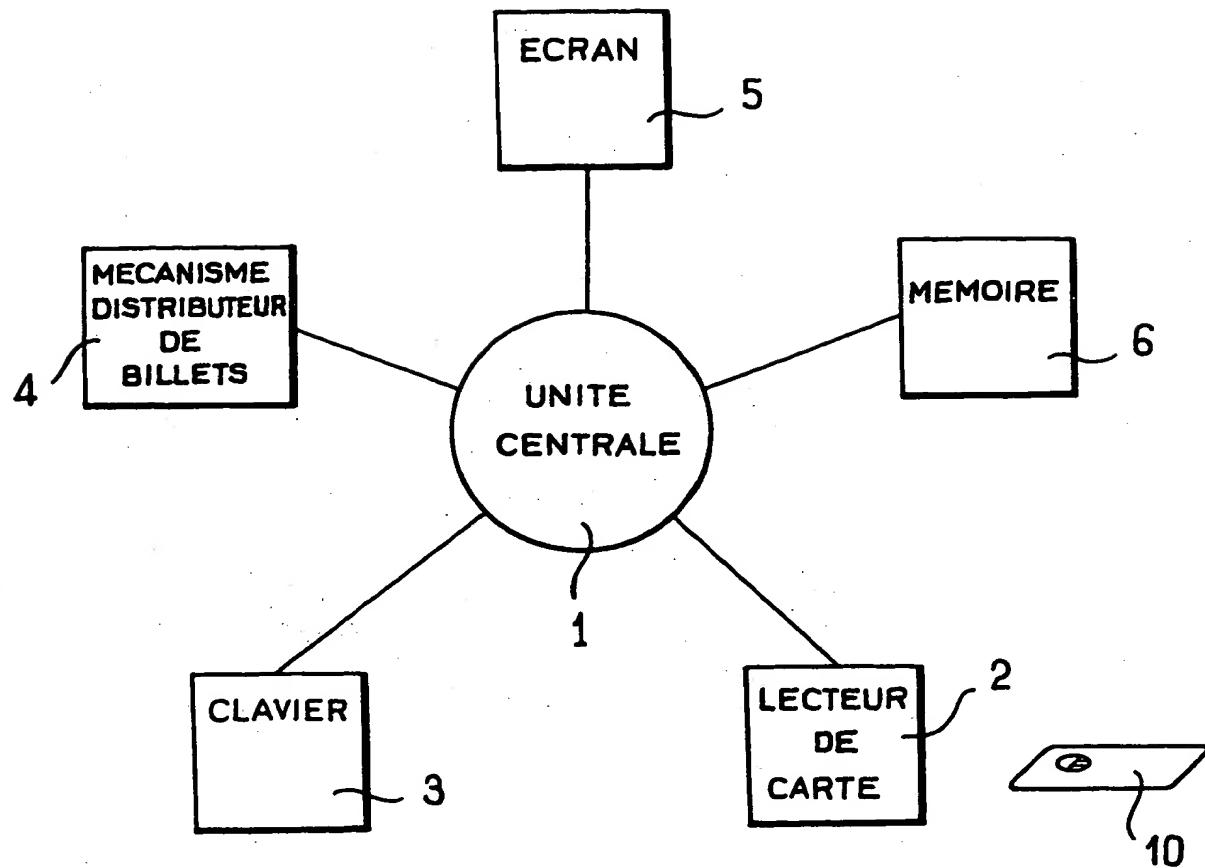


FIG.1

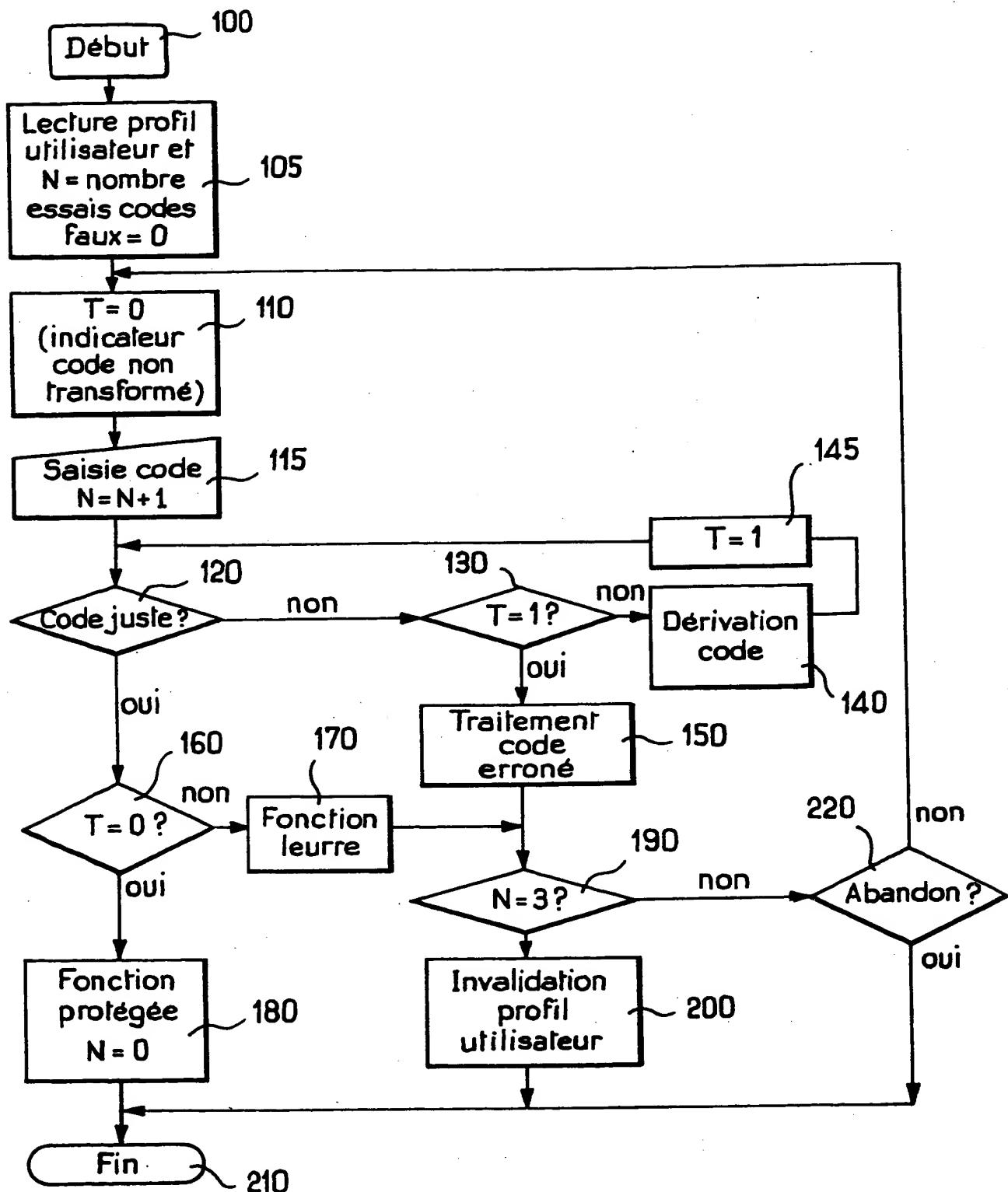


FIG. 2